BIUST Teaching, Research, & Innovation Symposium 2023 (TRDAIS 2023)
Botswana International University of Science and Technology
Palapye, Botswana, 18 - 19 September 2023
ISSN: 2521-2293

Development of an African National Cybersecurity Strategy Development Guide (ANCSDG): Botswana context

Violet Lebogang
Department of Computer Science and Information Systems
Botswana International University of Science and Technology
Palapye, Botswana
lv20100141@studentmail.biust.ac.bw

Oteng Tabona
Department of Computer Science and Information Systems
Botswana International University of Science and Technology
Palapye, Botswana
tabonao@biust.ac.bw

Thabiso Maupong
Department of Computer Science and Information Systems
Botswana International University of Science and Technology
Palapye, Botswana
maupongt@biust.ac.bw

***Abstract*—Botswana, like many other African countries, is undergoing a digital transformation. Whilst this transformation presents a vast amount of opportunities to greatly improve citizens' lives, there are associated risks. One of which is cybercrime. Cybercrime is a growing phenomenon that can not only disrupt businesses or personal systems but can also affect the national critical ICT infrastructure such as the supply of water, electricity, as well as business and government applications. Although efforts by the government have been made to secure the cyberspace through publishing a national cybersecurity strategy, establishing a cybersecurity incident response team, and adopting cybersecurity-related legal frameworks, a holistic approach to cybersecurity is still lacking and there is still a gap in terms of interoperability and shared understanding within the cybersecurity strategic environment. This research proposes the development of a semantic-based National Cybersecurity Strategy Development Guide (African National Cybersecurity Strategy Development Guide- ANCSDG). This ontology will help address the interoperability issues within the cybersecurity environment and it can also be used as a model for the development and implementation of the National Cybersecurity Strategy (NCS) in Botswana. The guide will be developed per the International Telecommunications Union (ITU) 's national cybersecurity development guide. The guide will cover six different components: Critical Infrastructure Protection, Governance, Cybercrime Reporting, and Intelligence, Risk Management, Regional and International Cooperation, Capacity, and capability building.**

Keywords—component; Cybersecurity; cybercrime; strategy development guide; security ontology

A. INTRODUCTION

Botswana is increasingly being targeted by cybercriminals. (Serianau, 2018). In an initiative to counter these attacks, the Government has formulated a national cybersecurity strategy that was approved by parliament in October 2020 (ITU, 2022). This strategy was developed by the Ministry of Transport and Communication in collaboration with other government and private stakeholders. International partners such as Great Britain Government's Foreign & Commonwealth Office and USA State Department through MITRE and Carnegie Mellon University also played a part in the development (Lebogang, Tabona and Maupong 2022). A national cybersecurity assessment was carried out in 2012 with the assistance of the ITU and International Multilateral Partnership Against Cyber Threats (IMPACT) to assess the country's readiness for establishing a National Incident Response Team (BwCIRT). Since then, Botswana has enacted cybersecurity-related laws like the Cybercrime and Computer-related crimes act of 2018, Data Protection Act of 2018, Consumer Protection Act of 2018, and Electronic Records (Evidence) Act of 2014, and it has also set up a Cybersecurity Incident Response Team.

Overall, the National Cybersecurity Strategy does not provide good evidence of a comprehensive assessment especially outlining the threat landscape and there is not much emphasis on using a holistic approach for the implementation of the NCS and how its progress will be monitored (Lebogang, Tabona, and Maupong 2022). On the Global Cybersecurity Index (GCI) report compiled by ITU in 2020, Botswana ranked 88th out of 198 countries globally and 12th of 43 countries in Africa. In another cybersecurity index compiled by e-Governance Academy, as of 2022, Botswana has been ranked 113th out of 160 countries globally. This is a decrease from the 100th ranking which was recorded in 2020. This indicates that there is low cyber maturity in the area. A strategy development guide is needed to help Botswana develop robust cybersecurity strategies.

Although various structures have been established to deal with cybersecurity in Botswana, they are still by e-

ISSN: 2521-2293

Governance Academy, as of 2022, Botswana has been ranked 113th out of 160 countries globally. This is a decrease from the 100th ranking which was recorded in 2020. This indicates that there is low cyber maturity in the area. A strategy development guide is needed to help Botswana develop robust cybersecurity strategies.

Although various structures have been established to deal with cybersecurity in Botswana, they are still inadequate and the implementation of the strategy is at an infant stage. Additionally, there is still a gap in terms of interoperability and shared understanding within the cybersecurity environment. (Rantos, 2021).

In trying to address this problem, Jansen van Vuuren et al. (2013) developed a cybersecurity policy implementation framework for South Africa. The framework is based on previous work by Jansen van Vuuren et al. (2012), an implementation framework proposed by Otoom & Atoum (2012), guidelines for the implementation of national cybersecurity strategies by Ghernouti-Helie (2010), and a cybersecurity Awareness toolkit by Phahlamohlaka et al., 2011.

This paper describes a semantic-based National Cybersecurity Strategy development guide to support Botswana in the development and implementation of a comprehensive and effective National Cybersecurity Strategy (NCS). This will map an ideal cybersecurity strategic environment. It will capture the complexity of the interactions required between different stakeholders to develop and implement a National Cybersecurity Strategy (NCS). The ultimate goal of this effort is to develop an ontology of the cybersecurity strategic environment expressed in OWL language. The availability of a formally encoded cybersecurity strategic environment will enable …

The rest of the document is structured as follows: section 2 will provide a brief literature review and related works. Section 3 will describe the methodology employed to develop the proposed solution, section 4 will describe the proposed model and the research will be concluded in section 5.

. RELATED WORKS

Despite the fact that several ontologies have been developed for the cybersecurity domain, the use of ontologies to model the complexities of cyber governance, in particular, has received limited attention in the research community. Greiman (2018) reflected on how ontological research methodologies contribute to the understanding of cyber governance at the global level. One of the numerous motivations the author highlights for using an ontology to model the complexity of the cyber governance environment is the ability of an ontology to formally define a vocabulary for the domain. Greiman found out that although there have been a number of research activities on the development of cybersecurity ontologies (Obrst, Chase, & Markeloff, 2021), there are very few investigations on the use of ontological development to support the interoperability of cyber governance at the international level. Greiman explored an ontological approach to analyze cyber governance with the motivation that ontological models can provide insight into the entities, attributes, and processes in this domain.

Previous works have used qualitative approaches including interviews and literature review to develop a national cybersecurity strategy development framework or provide suggestions for the improvement of the existing cybersecurity frameworks. Some of the works by J C Van Vuuren et al., 2013; Kulikova et al., 2012; K. 2012; and Amir Mohammed Talib et al., 2018 are discussed below;

.TABLE STYLES

Past related works in literature		
Researchers	***Methods***	***Findings***
J C Van Vuuren et al. (2013)	Literature review	This paper describes a cybersecurity policy implementation framework for South Africa which is based on previous work of the authors as well as guidelines and other frameworks in the literature.
J C Van Vuuren et al. (2019)	Literature review	This paper presents a framework for African countries to develop and implement a national cybercrime. It includes elements such as Governance, Cooperation, Reporting and Intelligence, Education and Awareness as well as High- tech crime and other specialized units.
Otoom & Atoum, 2012	Literature review	This paper proposes an implementation framework that lays out the ground for a coherent, systematic, and comprehensive approach to implementing the National Information Assurance and Cyber Security Strategy (NIACSS) of Jordan. The Framework 1). Suggests a methodology to analyze the NIACSS, 2). Illustrates how the NIACSS analysis can be utilized to design strategic moves and develop an appropriate functional structure, and 3). proposes a set of adaptable strategic controls that govern the NIACSS implementation and allow for achieving excellence, innovation, efficiency, and quality.
Khosraw Salamzada et al. (2015)	Qualitative approach using semi-structured interviews	This paper presented a framework for cybersecurity strategy for developing countries. This paper particularly focused on Afghanistan.
Kulikova (2012)	Interview and Literature review	This paper presented a cybersecurity framework and validated testing, defining two security incident scenarios and interviews.
Government of the Republic of South Africa		The National Cybersecurity Policy Framework (NCPF) proposed in this paper outlines policy guidelines related to

ISSN: 2521-2293

Past related works in literature		
Researchers	***Methods***	***Findings***
		cybersecurity in SA and requires the government to develop detailed cybersecurity policies and strategies. It aims to address national security in terms of cyberspace security, for example, cyber-warfare, cybercrime, cyber-terrorism, and cyber-espionage.

Table 1: Related works

B. ONTOLOGY CONSTRUCTION

In this section, the methodology that was employed for the development of the ANCSDG ontology is described.

. *Methodology*

In order to achieve the main objective of this research, which is to develop a semantic-based National Cybersecurity Strategy Development Guide (African National Cybersecurity Strategy Development Guide-ANCSDG), a research methodology proposed by (Fernández-López et al., 1997) called 'METHONTOLOGY' was used. This methodology is based on the idea of software engineering, which defines a set of tasks to be performed to develop a consistent and complete conceptual model. The authors of this paper also considered other methodologies like the one proposed by (Grüninger and Fox, 1995), (Noy and McGuinness, 2001), (Ahmed et al., 2007), and (Kumara, 2006) but because methontology is widely adopted, provides support in building ontologies from scratch, can be applied for the reuse of existing ontologies and it is flexible and easy to adopt. Below are the tasks that were followed to develop the ontology.

. *Specification*

The goal of the specification phase was to produce an informal ontology specification document written in natural language, using a set of competency questions. The technique used in the knowledge acquisition phase of the ANCSDG ontology was informal text analysis. Its purpose was to study the main concepts given in books and handbooks. This study enables you to fill in the set of intermediate representations of the conceptualization.

b. *Conceptualization*

In this activity, domain knowledge was structured in a conceptual model that describes the problem and its solution in terms of the domain vocabulary identified in the ontology specification activity. After most of the knowledge was acquired, there was a vast amount of unstructured knowledge that needed to be organized. Conceptualization organizes and structures the acquired knowledge using external representations that are independent of the implementation languages and environments. Specifically, this phase organizes and converts an informally perceived view of a domain into a semi-formal specification, using a set of intermediate representations that the domain expert and ontologist can understand. These IRs bridge the gap between how people think about a domain and the languages in which ontologies are formalized. This set of IRs is based on those used in the conceptualization phase of the ideal methodology for knowledge-based systems development.

The first task was to build a complete Glossary of Terms (GT). Terms include concepts, instances, verbs, and properties. So, the GT identifies and gathers all the useful and potentially usable domain knowledge and its meanings. Terms were further grouped as concepts and verbs. Each set of concepts/verbs included concepts/verbs that are closely related to other concepts/verbs inside the same group as opposed to other groups. For each set of related concepts and related verbs, a concepts classification tree and a verbs diagram are built.

After they have been built, the ontology development process was split into different but related, teams. Those related to concepts should follow the guidelines presented by G6mezPtrez and colleagues in (G6mez-Ptrez, Fern;indez, & De Vicente 1996), and those encharged of conceptualizing verbs are presented at (Vicente 1997). Concepts will be described using (G6mez-Ptrez, Fern;tndez, & De Vicente 1996): Data Dictionary, which describes and gathers all the useful and potentially usable domain concepts, their meanings, attributes, instances, etc.; tables of instance attributes, which provide information about the attribute or about its values at the instance; tables of class attributes, to describe the concept itselL, not its instances; tables of constants, used to specify information related to the domain of knowledge that always take the same value; tables of instances, which define instances; and attributes classification trees, to graphically display attributes and constants related in the inference sequence of the root attributes, as well as the sequence of formulas or rules to be executed to infer such attributes. Verbs represent actions in the domain. They could be described using (Vicente 1997): Verbs Dictionary, to express the meaning of verbs in a declarative way; tables of conditions, which specify a set of conditions to be satisfied before executing an action, or a set of conditions to be guaranteed after the execution of an action. Finally, to say that tables of formulas and tables of rules gather knowledge about formulas and rules. Note that both branches use these two intermediate representations.

c. *Integration*

Rather than building the ontology from scratch, the authors made use of some definitions that were already built into the ontology which was proposed by (van Vuuren et al., 2014). For the missed definition, justification and benefits of their inclusion are provided.

d. *Implementation*

Ontologies implementation requires the use of an environment that supports the meta-ontology and ontologies selected at the integration phase. During this stage, the ontology was codified in a formal language

ISSN: 2521-2293

called Ontology Web Language (OWL). The implementation environment that was chosen was protege desktop v5.5.0 software tool. Protégé is a free, open-source ontology editor and a knowledge management system.

e. Evaluation

Evaluation includes verification and validation. Verification refers to the technical process that guarantees the correctness of an ontology. Validation guarantees that the ontologies, software environment, and documentation correspond to the system they represent.

The output proposed by METHONTOLOGY for this activity is many evaluation documents in which the ontologist will describe how the ontology has been evaluated, the techniques used, the kind of errors found in each activity, and the sources of knowledge used in the evaluation.

In this research, a corpus based approach or data-driven approach will be used to evaluate the accuracy, conciseness and completeness of the NCSs.

f. Documentation

There are no set guidelines on how to document ontologies. In many instances tthe only documentation available is in the code of the ontology, the natural language text attached to formal definitions, and papers published in conference proceedings and journals setting out important questions of the ontology already built. In this research, documentation was done as an activity throughout the ontology development process.

C.

C. THe ANCSDG ONTOLOGY

This section has been divided into two parts. Subsection A gives a brief overview of what ontologies are and subsection B presents the ANCSDG ontology.

. *What is an ontology?*

In literature, there exist many definitions of what an ontology is. Noy and McGuinness (2001) describe ontology as “a formal explicit description of concepts of discourse classes, with the properties of each class describing various attributes of the concepts (slots) and their restrictions”. Other researchers describe ontology as a technology that provides a way to exchange semantic information between people and systems. However, in this research, the definition of ontology as described by Grüber (1993) will be adopted. Grüber (1993) defines an ontology as a “formal, explicit specification of a shared conceptualization”.

Ontologies provide many benefits, some of which is that they facilitate reuse of domain knowledge, they make domain assumptions clear, they separate domain knowledge from operational knowledge and they allow sharing of a common understanding of the structure of information.

This research will harness the power of ontologies to map an ideal cybersecurity strategic environment. The ANCSDG ontology will provide a single shareable model of the cybersecurity strategic environment. During the development and implementation of the cyber security strategy, the ontology can be used to map relevant aspects of the strategy to actors and functions as described in the ontology.

B. ANCSDG Ontology

This section describes the ANCSDG ontology. This ontology was developed as per ITU’s National Cybersecurity Strategy Development Guide and also a text corpus that was created using Sketch Engine. Sketch Engine is a corpus manager and text analysis software developed by Lexical Computing. The corpus and ITU’s strategy development guide were used to identify the main concepts of the ontological model as well as their subclasses.

The model was then implemented on Protege Desktop v5.5.0. Protege is a free, open-source ontology editor and a knowledge management system. The table below describes the logical axioms for the ANCSDG ontology.

Table 1 Axioms of the ANCSDG Ontology

Logical Axioms for the ANCSDG Ontology	
Concept name	***Axiom Description***
Governance	This component looks at laws and other technical structures developed by the government to secure cyberspace.
Risk Management	This component looks at structures and methods that have been put in place to manage cyber risks.
Capacity and Capability Building	This component looks at building local, regional and international cooperation among African countries.
Regional and International Cooperation	This component looks at efforts that have been put in place to support local, regional and international cooperation
Critical Infrastructure Protection	This component looks at the structure and measures that have been put in place to secure cyberspace.
Cybercrime Reporting and Intelligence	This component looks at cybercrime reporting and intelligence gathering and sharing.

ISSN: 2521-2293

Axioms provide a formal way to add logical expressions to an ontology. These logical expressions can be used to refine the concepts and relationships in the ontology. Axioms are used to design an explicit way of expression that is always true. Axioms can be used for defining the meaning of several components of the ontology, defining complex relationships and verifying the correctness of the information of obtaining new information. Table shows some of the axioms on the ANCSDG ontology.

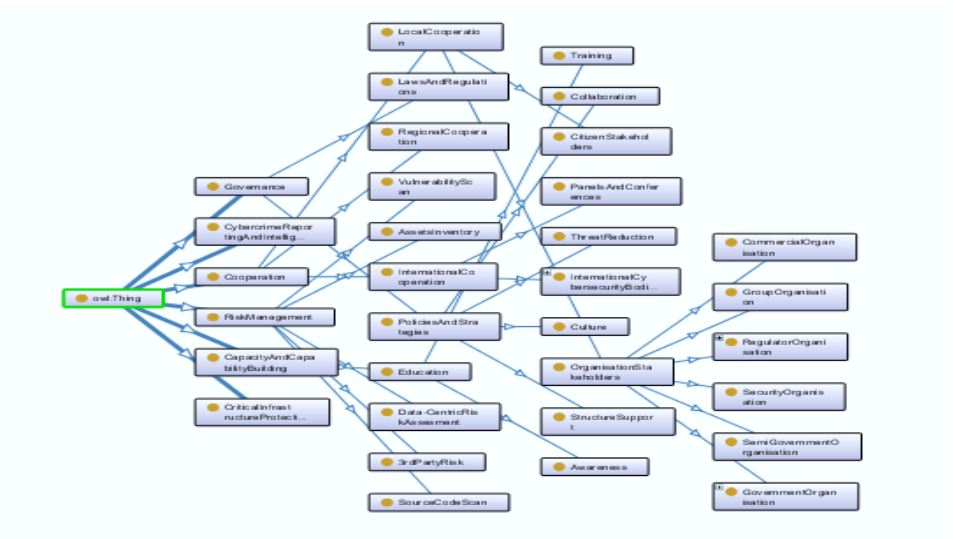

Fig. 1. The ANCSDG Ontology

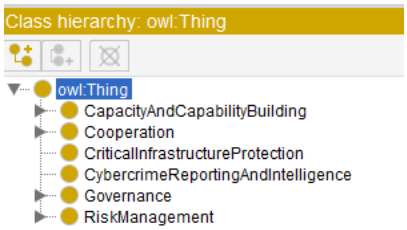

Figure 1 Main Concepts of the ANCSDG Ontology

Figure 1 above describe the main concepts of the ANCSDG ontology. These concepts were extracted from different relevant published papers, the Cybersecurity Policy Implementation ontology (CPIO) by and the ITU's cybersecurity development guide.

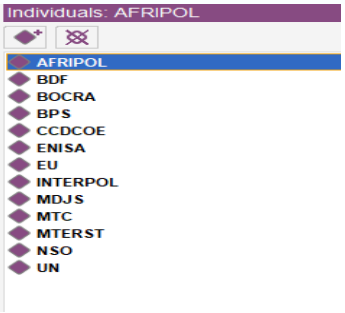

Fig. 2. In of the ANCSDG Ontology

Figure 2 above describes individuals of the ANCSDG ontology. Individuals or instances represent the objects in the domain. In this study, the individuals represent the different stakeholders that are relevant to NCS development and implementation. Figure 4 shows some individuals of the ANCSDG ontology.

ISSN: 2521-2293

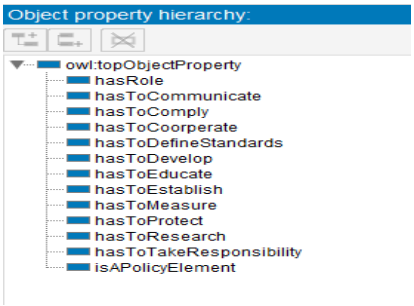

Fig. 3. Object properties of the ANCSDG

Figure 3 above describes the object properties of the ANCSDG ontology. Object properties refer to the relationships among concepts.

B. CONCLUSIONS

In this paper, the authors presented a semantic-based cybersecurity strategy development guide (ANCSDG) that is tailored to support Botswana in the development and implementation of a comprehensive National Cybersecurity Strategy (NCS). The first task was to assess existing solutions and their shortcomings. Thereafter, an ontology mapping the cybersecurity domain was implemented on Protégé Desktop v5.5.0. This ontology was developed as per ITU's National Cybersecurity Strategy Development guide. In addition to ITU's development guide, a text corpus that was created using the Sketch Engine was also utilized. The availability of a formal, encoded description of the cybersecurity strategic environment allows policymakers and other stakeholders that are relevant to the development of the NCS to identify which concepts are critical in NCS formulation and also how these concepts are related to one another. During the implementation of the strategy, the model will be used to map relevant aspects of the strategy to actors and functions as described in the ontology. Furthermore, an ontology for the cybersecurity strategic environment will help deal with issues of interoperability and knowledge sharing in the cybersecurity strategic environment. To the best of our knowledge, there only exists one other solution of this kind in the literature and the main difference between the presented solution and the one that already exists is the addition of new concepts, relationships, and data properties. These components were necessary for a holistic approach to the development and implementation of NCSs. Although this solution was initially developed for Botswana, it is applicable to be used by other African countries.

ACKNOWLEDGMENT

I would like to thank my supervisors and everyone who contributed to the successful completion of this research.

REFERENCES

[1] Serianu, (2018), African Cybersecurity Report- Botswana, Retrieved on September 22 from: https://africancyber.com/Botswana%20Cyber%20Crime%20Report%202018-2019.pdf

[2] Cybersecurity Capacity Centre for Southern Africa (C3SA), (2021), Southern African Development Community Cybersecurity Maturity Report 2021, Retrieved on September 22 from:https://open.uct.ac.za/bitstream/handle/11427/36211/SADC%20CYBERSECURITY%20CAPACITY%20MATURITY%20REPORT%202021.pdf?sequence=5

[3] Jansen van Vuuren, J.C., Leenen, L., Phahlamohlaka, L.J. and Zaaiman, J.J., 2013. Development of a South African cybersecurity policy implementation framework. Academic Conferences and Publishing International.

[4] Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C. and Katos, V., 2020. Interoperability challenges in the cybersecurity information sharing ecosystem. *Computers*, *9*(1), p.18.

[5] Atoum, I., Otoom, A. and Ali, A.A., 2014. A holistic cyber security implementation framework. *Information Management & Computer Security*.

[6] Salamzada, K., Shukur, Z. and Bakar, M.A., 2015. A framework for cybersecurity strategy for developing countries: Case study of Afghanistan. *Asia-Pacific Journal of Information Technology and Multimedia*, *4*(1), pp.1-10.

[7] South Africa Government Information. (2012). Statement on the Approval by Cabinet of the Cybersecurity Policy Framework for South Africa. Retrieved on 21 October 2012 from http://www.info.gov.za/speech/DynamicAction?pageid=461&sid=25751&tid=59794

[8] Gcaza, N., von Solms, R. and van Vuuren, J.J., 2015. An Ontology for a National Cyber-Security Culture Environment. In *HAISA* (pp. 1-10).

[9] Lebogang, V., Tabona, O. and Maupong, T., 2022. Evaluating Cybersecurity Strategies in Africa. In *Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security* (pp. 1-19). IGI Global.

[10] Fernández-López, M., Gómez-Pérez, A. and Juristo, N., 1997. Methontology: from ontological art towards ontological engineering.

[11] Grüninger, M. and Fox, M.S., 1995. Methodology for the design and evaluation of ontologies.

[12] Noy, N.F. and McGuinness, D.L., 2001. Ontology development 101: A guide to creating your first ontology.

[13] Nanda, J., Simpson, T.W., Kumara, S.R. and Shooter, S.B., 2006. A methodology for product family ontology development using formal concept analysis and web ontology language.

[14] Ahmed, S., Kim, S. and Wallace, K.M., 2007. A methodology for creating ontologies for engineering design.

[15] Fernández-López, M., Gómez-Pérez, A. and Juristo, N., 1997. Methontology: from ontological art towards ontological engineering.

[16] Van Vuuren, J.J., Leenen, L. and Zaaiman, J., 2014, March. Using an ontology as a model for the implementation of the National Cybersecurity Policy Framework for South Africa. In *9th International Conference on Cyber Warfare and Security* (pp. 107-115).

[17] Raad, J. and Cruz, C., 2015, November. A survey on ontology evaluation methods. In *Proceedings of the International Conference on Knowledge Engineering and Ontology Development, part of the 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*.

[18] Protégé. The Prot´eg´e project, http://protege.stanford.edu, (2002)

[19] Gruber, T.R., 1993. A translation approach to portable ontology specifications. *Knowledge acquisition*, *5*(2